U.S. CONVENTIONAL PATENT APPLICATION
Attorney's Docket No: 3521

Certification of Express Mailing (37 C.F.R. Section 1.10)
I hereby certify that this Conventional Patent Application is being deposited with the United States Postal Service as "Express Mail Post Office to Addressee" Number EV307933714US on the date below in an envelope with sufficient postage addressed to: MS Patent Application, Commissioner for Patents, PO Box 1450, Alexandria, VA 22313-1450.
Printed or Typed Name: BARBARA S PEDERSEN
Signature: Barbara S Pedersen
Date of Deposit: July 22, 2003

A method of message modification in a communication system and a device for performing the method

Description

This application claims priority from, and is a continuation-in-part of, prior application number 09/857,072, issuing as Patent No. 6,597771 on July 22, 2003, which is a 35 U.S.C. 371 application of PCT/CZ99/00048, the disclosure of which is herein incorporated by this reference.

Technical field

The invention relates to a method of message modification in a communication system and a device for performing the method, the communication system including at least one transmitter communication unit, data communication means and at least one receiver communication unit, and the message modification being performed after the message has been sent from a home communication unit to a target one.

Background of the invention

There are known communication systems comprising a transmitter communication unit, data communication means and a receiver communication

unit. Communication units may be both mobile and fixed. E.g. in an electronic-mail system, there are systems working in such a manner, that a created message, an electronic document, is by means of a computerized system, operating as data communication means, transmitted at first to a server of a provider of the connection and then to a mail server of an Addressee. The electronic message shall be stored in the mail server, until it is withdrawn by the addressee.

By analogy, by transmission of audio messages and/or those in a text form, within the framework of a communication system, there is at one side created an audio and/or text message, which is by means of data communication means, such as a telephone network portable or fixed radio facilities, cellular wireless telephone devices etc., transmitted to a receiver communication unit, e.g. a telephone or a fax recorder.

In each case, from the moment of sending an electronic document and/or a message in audio or text from the transmitter communication unit, the sender has no possibility to modify and/or delete the message, in spite of the fact that the addressee has not withdrawn or read the message yet. If the sender later wishes to hand over some information that differs from that one included in the document delivered previously, he has only one possibility to do so, that is, to send another document referring to the original one

It is an object of the invention to provide a method for a modification of a message which has already been sent away.

Disclosure and Object of the Invention

The object of the invention is achieved and the foregoing problems are solved by a method of a message modification in a communication system including at least one transmitter communication unit, data communication means and at least one receiver communication unit in accordance with the present invention comprising a procedure in which after receiving a message, the message being delivered into a receiver communication unit through data communication means and stored in a storage unit, there is a password allocated to the sender, the password being allocated with respect to available information about an identity of the sender, and the password is delivered back to the transmitter communication unit as acknowledgement message and serves the

sender as a key for obtaining an access to functions for modification and/or deleting a message stored in the receiver communication unit. Besides the access password there may be also delivered other information the receiver wants to pass to the sender.

Alternative embodiments of the invention include other means for identifying the sender with a specific message and for allowing the sender to modify, delete, retrieve the message before withdrawal by the receiver. For example,

- A password does not necessarily need to be sent by the receiver, but instead can be generated by the sending equipment and communicated to the receiving equipment
- The receiver may use a different method for identifying the sender with the message. The different method may be based on cryptographic technology known as "Public Key" or "Asymmetric Key" or "Digital Signature". In such a case a password would not be sent by the receiver but instead the identification would be executed using information provided by the sender.
- The same or similar processes of communication with and identification of the sender can also be used to discern between legitimate messages and "Unsolicited Commercial Messages" a.k.a. "Spam". This detection of Spam may be based on the fact that "Spammers" would be impossible to identify because they would not respond to communication and/or their email address would not be functional, and/or they would not have a trustworthy digital signature.
- The inventor envisions that many different methods and apparatus for identifying the sender with a message and allowing access to the message may be designed, keeping with the intended goals of the invention as herein mentioned.

Further in accordance with the invention the received message is analyzed, and provided its parameters differ from required ones, the sender is invited to modify the message. Still in accordance with the invention there is created an archive copy of a delivered message, which by means of the access password has been modified and/or deleted by the sender. According to another aspect of

the invention there is provided an equipment for performing the said method, the equipment including at least one transmitter communication unit, data communication means and at least one receiver communication unit, where the data communication means comprise computerized system, preferably an Internet computer network. According to another preferred feature of this aspect of the invention the transmitter and/or receiver communication unit comprise an electronic unit and/or a system of electronic units, preferably a computer. Further in accordance with a preferred feature of the invention the data communication means comprise telecommunication means. Still in accordance with a preferred feature of the invention the transmitter and/or receiver communication unit comprise telephone and/or fax devices .

The method of modification of a message after being sent from a home communication unit through a communication system to a target communication unit facilitates a solution of the situation where the sender has dispatched an incorrect message, or where from the time of dispatching the message to its withdrawal by an addressee, conditions have altered so much that the said message has lost its validity. In such a case this invention allows the sender to change or delete the message without bothering the addressee with an unvalid message.

The subject of this invention brings further advantages in cases where a message in some its characteristic features, like structured information such as an electronic signature, theme classification according a given standard, file number, etc., does not meet the addressee´s demands. The communication unit of the addressee analyses the received message and the modification system according to the invention allows the sender to demand completion and/or modification of the message even before the addressee is able to withdraw it.

The subject of this invention brings further advantages in cases where it is needed to discern between legitimate messages and "Unsolicited Commercial Messages" or Spam.

Description of examples of invention execution

First Example

There is described a modification of an electronic message in a communication system, namely within a framework of a message exchange through the Internet computer network.

As a transmittion and/or a receiver communication unit there is aplied an electronic unit such as computer and comprise input and output units and is connected to a storage unit, e.g. a mail server.

As data communication means there is used a computerized system such as the Internet computer network.

The sender dispatches a message from his computer and the message is through the Internet network delivered to a receiver mail server. The receiver communication unit allocates an access pasword to the received message the decision about the access password allocation being based upon available information about the identity of the sender.

Within the receiver communication unit it is possible to set more programs, advantageously two programs for edition and allocation of access passwords. The first program provides for edition of a new password for each received message irrespective to the identity of the sender.

In the other case the identity of the sender is taken into account. Provided the identity is unknown to the receiver communication unit, which means the identity is a new one, there is a new access pasword edited for this sender. On the contrary, the identity being known to the receiver unit, which means the sender has previously transmitted any message to the receiver unit and has therefore already received his personal access password, the receiver unit decides not to allocate a new password and the sender may further modify his messages using the original access password.

The edited access password as a return message is sent by the receiver communication unit back to the transmitter communication unit. The return message including the access password may comprise also further information the addressee wishes to pass to the sender.

The access password enables the sender to modify and/or cancel the message stored at the receiver mail server and has not been withdrawn yet.

Alternative embodiments of the invention include other means for identifying the sender and for allowing the sender to modify, delete, retrieve the message before withdrawal by the receiver. For example,

- A password does not necessarily need to be sent by the receiver, but instead can be generated by the sending equipment and communicated to the receiving equipment
- The receiver may use a different method for identifying the sender with the message. The different method may be based on cryptographic technology known as "Public Key" or "Asymmetric Key" or "Digital Signature". In such a case a password would not be sent by the receiver but instead the identification would be executed using information provided by the sender.
- The same or similar processes of communication with and identification of the sender can also be used to discern between legitimate messages and "Unsolicited Commercial Messages" a.k.a. "Spam". This detection of Spam may be based on the fact that "Spammers" would be impossible to identify because they would not respond to communication and/or their email address would not be functional, and/or they would not have a trustworthy digital signature.
- The inventor envisions that many different methods and apparatus for identifying the sender with a message and allowing access to the message may be designed, keeping with the intended goals of the invention as herein mentioned.

As an optional function the receiver communication unit may in a further step analyze the received message and when having found its parameters unsatisfactory or different from desired ones it demands the sender to modify the message.

As another optional function the receiver communication unit creates an archive copy of the original message which has been later modified or erased by the sender using his access password.

The Second Example

There is described a method of a modification of an audio message and/or a text message in a communication system, in which the transmitter communication unit and/or the receiver ones are provided for by an electronic unit and/or a telephone set and/or a facsimile device and a telecommunication means are represented by the data communication means.

The sender dispatches a message, e.g. an audio message from his communication unit and the message is delivered to the receiver communication unit where it is recorded in a storage unit. The receiver communication unit allocates an access password, the allocation being based upon available information about identity of the sender

Within the receiver communication unit it is possible to set more programs, advantageously two programs for edition and allocation of access passwords. The first program provides for edition of a new password for each received message irrespective to the identity of the sender. In this case there may be used even a simple receiver communication unit, such as a telephone recorder, which performs no identification of the sender and immediately issues an access password for each delivered message.

In the other case the indentity of the sender is taken into account. Provided the identity is unknown to the receiver communication unit, which means the identity is a new one, a new acces pasword is edited for this sender. On the contrary the identity being known to the receiver unit, which means the sender has previously transmitted messages to the receiver unit and has therefore already received his personal access password, the receiver unit decides not to allocate a new password and the sender may modify his further messages using the original access password.

The edited access password as a return message is send by the receiver communication unit back to the transmitter communication unit. The return message including the access password may comprise also further information the addressee wishes to pass to the sender.

The access password allows the sender to modify and/or cancel the message stored at the receiver mail server and has not been withdrawn yet.

Alternative embodiments of the invention include other means for identifying the sender and for allowing the sender to modify, delete, retrieve the message before withdrawal by the receiver. For example,

- A password does not necessarily need to be sent by the receiver, but instead can be generated by the sending equipment and communicated to the receiving equipment
- The receiver may use a different method for identifying the sender with the message. The different method may be based on cryptographic technology known as "Public Key" or "Asymmetric Key" or "Digital Signature". In such a case a password would not be sent by the receiver but instead the identification would be executed using information provided by the sender.
- The same process of communication with and identification of the sender can also be used to discern between legitimate messages and "Unsolicited Commercial Messages" a.k.a. "Spam". This detection of Spam may be based on the fact that "Spammers" would be impossible to identify because they would not respond to communication and/or their email address would not be functional, and/or they would not have a trustworthy digital signature.
- The inventor envisions that many different methods and apparatus for identifying the sender with a message and allowing access to the message may be designed, keeping with the intended goals of the invention as herein mentioned.

As an optional function the receiver communication unit may in a further step analyze the received message and when founding its parameters unsatisfactory or different from desired ones it demands the sender to modify the message.

As another optional function the receiver communication unit creates an archive copy of the original message which has been later modified or erased by the sender using his access password.

Industrial applications

The method of message modification in the communication system after its dispatching from the home communication unit to a target one is applicable in fields of computer and/or telecommunication techniques, namely for electronic mail systems and in such a case, the interchange of messages should be realized under variable circumstances requiring some modifications of already delivered messages.

Although this invention has been described above with reference to particular means, materials, and/or embodiments, it is to be understood that the invention is not limited to these disclosed particulars, but extends instead to all equivalents within the scope of the following claims.